(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－353958
（P2002－353958A）
(43)公開日　平成14年12月６日(2002.12.6)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード*(参考)
Ｈ０４Ｌ　9/32		Ｂ４２Ｄ　15/10	５０１Ｅ	２Ｃ００５
Ｂ４２Ｄ　15/10	５０１		５１１	５Ｂ０８５
	５１１		５２１	５Ｊ１０４
	５２１	Ｇ０６Ｆ　15/00	３３０Ｂ	
Ｇ０６Ｆ　15/00	３３０	17/60	２２２	

審査請求　未請求　請求項の数24　ＯＬ　（全 17 頁）　最終頁に続く

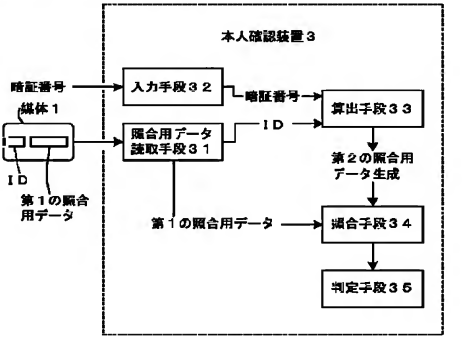
(21)出願番号　特願2001－153854(P2001－153854)
(22)出願日　平成13年５月23日(2001.5.23)

(71)出願人　598049322
株式会社東京三菱銀行
東京都千代田区丸の内２丁目７番１号
(72)発明者　飯坂　俊治
東京都千代田区丸の内２丁目７番１号　株式会社東京三菱銀行内
(74)代理人　100086863
弁理士　佐藤　英世

最終頁に続く

(54)【発明の名称】　本人確認方法、本人確認装置、媒体作成装置、媒体、媒体保管情報の処理方法、プログラム及び記録媒体

(57)【要約】
【課題】　他の装置との接続が要求されることなく媒体単体で本人確認が完結でき、しかも本人確認のために入力される情報を媒体上にそのまま格納せずに、正確な本人確認が行える本人確認方法を提供せんとするものである。
【解決手段】　ユーザＩＤと暗証番号のデータ列に対してハッシュ関数により処理して得られる第１の照合用データ及び上記ユーザＩＤの記録された媒体１から、第１の照合用データ及びユーザＩＤが読み取られると共に、読み取られたユーザＩＤと入力された暗証番号のデータ列に対して上記と同じハッシュ関数によって第２の照合用データが算出され、該第２の照合用データと前記第１の照合用データとが照合されることで、本人確認が行われる。



【特許請求の範囲】
【請求項１】　少なくとも暗証データに対して一方向性関数により処理して得られる第１の照合用データの記録された媒体から、コンピュータ上に第１の照合用データが読み取られると共に、入力された暗証データに対し上記と同じ一方向性関数によって第２の照合用データが算出され、該第２の照合用データと前記第１の照合用データとが照合されることで、本人確認が行われることを特徴とする本人確認方法。
【請求項２】　ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、コンピュータ上に第１の照合用データ及びユーザデータが読み取られると共に、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第２の照合用データが算出され、該第２の照合用データと前記第１の照合用データとが照合されることで、本人確認が行われることを特徴とする本人確認方法。
【請求項３】　前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを用いることを特徴とする請求項１又は請求項２記載の本人確認方法。
【請求項４】　少なくとも暗証データに対して一方向性関数により処理して得られる第１の照合用データの記録された媒体から、第１の照合用データを読み取る照合用データ読み取り手段と、
暗証データの入力手段と、
入力された暗証データに対して上記と同じ一方向性関数によって第２の照合用データを算出する算出手段と、
上記第２の照合用データと前記第１の照合用データとを照合する照合手段と、
上記照合結果に基づき、本人か否かの判定を行う判定手段とを有することを特徴とする本人確認装置。
【請求項５】　ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、第１の照合用データ及びユーザデータを読み取る照合用データ読み取り手段と、
暗証データの入力手段と、
読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第２の照合用データを算出する算出手段と、
上記第２の照合用データと前記第１の照合用データとを照合する照合手段と、
上記照合結果に基づき、本人か否かの判定を行う判定手段とを有することを特徴とする本人確認装置。
【請求項６】　前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを用いることを特徴とする請求項４又は請求項５記載の本人確認装置。
【請求項７】　少なくとも暗証データが与えられることにより一方向性関数により処理して第１の照合用データを算出する演算手段と、
該第１の照合用データを媒体に書き込む照合用データ書き込み手段とを有することを特徴とする媒体作成装置。
【請求項８】　ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列が与えられることにより一方向性関数により処理して第１の照合用データを算出する演算手段と、
該第１の照合用データを媒体に書き込む照合用データ書き込み手段とを有することを特徴とする媒体作成装置。
【請求項９】　前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを用いることを特徴とする請求項７又は請求項８記載の媒体作成装置。
【請求項１０】　暗証データに対して一方向性関数により処理して得られる第１の照合用データを格納するための領域を有することを特徴とする媒体。
【請求項１１】　ユニークなユーザデータと暗証データを構成要素とするデータ列に対して一方向性関数により処理して得られる第１の照合用データを格納するための領域を有することを特徴とする媒体。
【請求項１２】　前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを用いることを特徴とする請求項１０又は請求項１１記載の媒体。
【請求項１３】　少なくとも暗証データに対して第１の一方向性関数により処理して得られる第１の照合用データの記録された媒体から、第１の照合用データが読み取られ、入力された暗証データに対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致したことにより、該保管情報と第３の照合用データとが記録されたという経緯を有する上記媒体から、コンピュータ上に第１の照合用データ、第３の照合用データ及び上記保管情報が読み取られるステップと、
別途入力された暗証データに対し上記第１の一方向性関数によって第４の照合用データが算出されるステップと、
第４の照合用データと読み取られた前記第１の照合用データとが照合されるステップと、

読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データが算出されるステップと、
上記照合ステップで第４の照合用データと第１の照合用データとが一致したことを条件として、読み取られた前記第３の照合用データと上記第５の照合用データとが照合されるステップと、
第３の照合用データと第５の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行することを特徴とする媒体保管情報の処理方法。

【請求項１４】　ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第１の一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、第１の照合用データ及びユーザデータが読み取られ、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致したことにより、該保管情報と第３の照合用データとが記録されたという経緯を有する上記媒体から、コンピュータ上にユーザデータ、第１の照合用データ、第３の照合用データ及び上記保管情報が読み取られるステップと、
別途入力された暗証データ及び読み取られた上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第４の照合用データが算出されるステップと、
第４の照合用データと読み取られた前記第１の照合用データとが照合されるステップと、
読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データが算出されるステップと、
上記照合ステップで第４の照合用データと第１の照合用データとが一致したことを条件として、読み取られた前記第３の照合用データと上記第５の照合用データとが照合されるステップと、
第３の照合用データと第５の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行することを特徴とする媒体保管情報の処理方法。

【請求項１５】　前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを用いることを特徴とする請求項１３又は請求項１４記載の媒体保管情報の処理方法。

【請求項１６】　少なくとも暗証データに対して第１の一方向性関数により処理して得られる第１の照合用データを格納するための第１の格納領域と、
該格納領域に第１の照合用データの記録された状態から、該照合用データが読み取られ、入力された暗証データに対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致した場合に格納される、該保管情報ための第２の格納領域と第３の照合用データのための第３の格納領域とを有することを特徴とする媒体。

【請求項１７】　ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第１の一方向性関数により処理して得られる第１の照合用データを格納するための第１の格納領域と、
上記ユーザデータを格納するための第２の格納領域と、これらの格納領域に第１の照合用データ及びユーザデータの記録された状態から、第１の照合用データ及びユーザデータが読み取られ、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致した場合に格納される、該保管情報ための第３の格納領域と第３の照合用データのための第４の格納領域とを有することを特徴とする媒体。

【請求項１８】　前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを用いることを特徴とする請求項１６又は請求項１７記載の媒体。

【請求項１９】　コンピュータに、
少なくとも暗証データに対して一方向性関数により処理して得られる第１の照合用データの記録された媒体から、第１の照合用データを読み取らせるステップと、
入力された暗証データに対し上記と同じ一方向性関数によって第２の照合用データを算出させるステップと、
該第２の照合用データと前記第１の照合用データとを照合させ、本人確認を行うステップとを実行させることを特徴とするプログラム。

【請求項２０】　コンピュータに、
ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理し

て得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、第１の照合用データ及びユーザデータを読み取らせるステップと、
読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第２の照合用データを算出させるステップと、
該第２の照合用データと前記第１の照合用データとを照合させ、本人確認を行うステップとを実行させることを特徴とするプログラム。
【請求項２１】　コンピュータに、
少なくとも暗証データに対して第１の一方向性関数により処理して得られる第１の照合用データの記録された媒体から、第１の照合用データが読み取られ、入力された暗証データに対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致したことにより、該保管情報と第３の照合用データとが記録されたという経緯を有する上記記体から、第１の照合用データ、第３の照合用データ及び上記保管情報を読み取らせるステップと、
別途入力された暗証データに対し上記第１の一方向性関数によって第４の照合用データを算出させるステップと、
第４の照合用データと読み取られた前記第１の照合用データとを照合させるステップと、
読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データを算出させるステップと、
上記照合ステップで第４の照合用データと第１の照合用データとが一致したことを条件として、読み取られた前記第３の照合用データと上記第５の照合用データとを照合させるステップと、
第３の照合用データと第５の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行させることを特徴とするプログラム。
【請求項２２】　コンピュータに、
ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第１の一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、第１の照合用データ及びユーザデータが読み取られ、入力された暗証データ及び上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致したことにより、該保管情報と第３の照合用データとが記録されたという経緯を有する上記媒体から、ユーザデータ、第１の照合用データ、第３の照合用データ及び上記保管情報を読み取らせるステップと、
別途入力された暗証データ及び読み取られた上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第４の照合用データを算出させるステップと、
第４の照合用データと読み取られた前記第１の照合用データとを照合させるステップと、
読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データを算出させるステップと、
上記照合ステップで第４の照合用データと第１の照合用データとが一致したことを条件として、読み取られた前記第３の照合用データと上記第５の照合用データとを照合させるステップと、
第３の照合用データと第５の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行させることを特徴とするプログラム。
【請求項２３】　前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを用いることを特徴とする請求項１９～請求項２２いずれか１つに記載のプログラム。
【請求項２４】　請求項１９～請求項２３のいずれかのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、セキュリティを高めた本人確認方法、本人確認装置、媒体作成装置、該媒体作成装置で作成され前記本人確認装置に用いられる媒体、その媒体に保管された情報の処理方法、これらのプログラム及び記録媒体に関する。
【０００２】
【従来の技術】これまでの本人確認方法の１つとして、磁気カードやＩＣカードなどの媒体を使用するものがある。このような構成の場合は、媒体の所有者によって、この媒体に関連する特定の情報が入力されることで行われる。
【０００３】上記本人確認の際入力される情報には、ユニークな（２つと無い）ユーザＩＤや暗証番号などがあり、通常これらの情報は、媒体中にも格納され、本人確認の都度、該媒体中から読み出されて、入力される情報

との突き合わせ処理が実施される。

【0004】すなわち金融機関などと取引を行うサービスで利用される媒体には、磁気カードやICカードなどが使用されている。そのうち①キャッシュカード・デビットカードなどの媒体による取引では、媒体の所有者（口座保有者）が、ATM、POS端末等で機器操作を行う場合、本人のみが知る暗証番号（通常4桁の数字）を機器に対して入力する。機器はカードより読み取った「データ」及び入力された「暗証番号」を1つの電文として送信し、発行体のホストコンピュータにおいて、入力された暗証番号が登録されたものと同一かどうかを照合し、本人確認を行う。

【0005】また②ICカードなどを使用するICクレジット取引・電子マネー取引等では、利用者がICクレジットカードを利用する都度、或いは電子マネー等を使って「小額な」支払いをする都度、入力された暗証番号と、ICカードに登録された「暗証番号」とをICチップ上で照合し、ホストに接続することなく、本人確認を行うスキームが存在する。この場合、利用ごとにホストコンピュータに接続しない（オフライン処理）ため、通信料金、データ処理料金等のコストが節減できる。

【0006】

【発明が解決しようとする課題】ところが、媒体中にこのような暗証番号などの情報が格納されていると、これらの情報解析を行うハッキング技術の標的になる場合が多い。このようなことは、磁気カードばかりか、一般に解析が難しいとされる上記ICカードなどの媒体でも同じである。

【0007】これに対し、セキュリティを高めるために、以上の情報のうち暗証番号については、媒体への格納が行われず、特定の装置と接続された際に、該暗証番号の入力が要求され、オンラインで本人確認がなされるようにすることも考えられる。

【0008】しかし、本人確認の際に常に特定の装置との接続が要求されるとなると、利用者側に余計な負荷がかかるなど、使い勝手が悪くなる。特にICカードなどに特定の金銭的価値を有するデータを格納させて電子通貨として使用する場合、支払の都度、特定のサーバへの接続が行われて、本人確認が実施されるようにしたのでは、電子通貨の利便性が損なわれることにもなりかねない。また特定のサーバへのトラフィックが増大し、各処理の本人確認が終了するまでに時間がかかってしまうことも想定される。

【0009】他方、「JAVA（登録商標）カード」、「MULTOSカード」、或いは「スマートカード for WINDOWS（登録商標）」などの汎用OSカードと呼ばれるカードは、後からソフトウェアなどの情報をカード上に書き込み・格納できる機能を有している。その場合にそれらの情報を書き込める者を確認する必要があるが、そのような情報の書き込みは、権限を与えられた特定のソフトウェアができるのみで、「権限の与えられた人間」ができるというものではない。ましてや書き込まれた情報を利用しようとする人物が、カードなどの媒体の正しい所有者乃至該媒体に情報を記録した者であるなどといった照合が行われたり、その内容に改竄がないなどの確認がなされることは保証されていない。

【0010】本発明は、以上のような問題に鑑み創案されたもので、他の装置との接続が要求されることなく媒体単体で本人確認が完結でき、しかも本人確認のために入力される情報を媒体上にそのまま格納せずに、正確な本人確認が行える本人確認方法、本人確認装置、媒体、媒体保管情報の処理方法、プログラム及び記録媒体を提供せんとするものである。

【0011】また媒体上に任意の情報が書き込まれてそれが利用できる構成において、書き込まれた情報を利用しようとする人物が、媒体の正しい所有者乃至該媒体に情報を記録した者であるなどといった照合ができ、しかもその内容に改竄がないなどの確認ができるような構成についても、併せて提案せんとするものである。

【0012】

【課題を解決するための手段】本発明は、少なくとも暗証データに対して、ハッシュ関数などの一方向性関数（処理結果から元データを割り出すことができない或いは難しい関数）により処理して得られる第1の照合用データの記録された媒体から、コンピュータ上に第1の照合用データが読み取られると共に、入力された暗証データに対し上記と同じ一方向性関数によって第2の照合用データが算出され、該第2の照合用データと前記第1の照合用データとが照合されることで、本人確認が行われることを基本的特徴としている。

【0013】上記構成によれば、媒体中に格納されるデータは、暗証番号などの暗証データそのものではなく、一方向性関数により処理して得られる第1の照合用データであり、そのため、仮に媒体からこれらのデータが読み出せたとして、第1の照合用データからは、暗証データを割り出す（推測する）ことはできない。従って本人確認の際に暗証データの入力を要求することで、入力された暗証データに対し上記と同一の一方向性関数で処理し、その結果得られた第2の照合用データと、前記媒体より読み取った第1の照合用データとの突き合わせを行い、その照合結果で本人確認処理を行えば、他の装置との接続が要求されることなく媒体単体で本人確認が完結できることになる。また媒体上に格納されるデータは、本人確認のために入力される情報そのものではなく、しかも媒体上に格納されるデータからは、上記入力の要求されるデータの割り出しが困難なため、セキュリティも向上することになる。すなわち、ユーザ以外は、いかなる者も真の暗証データを目にすることなく安全に媒体が作成され、媒体の盗難、偽造などに対しても、極めて強

力に対抗できるセキュリティを提供することができるようになり、さらに郵送中や媒体発行者の業務遂行中、或いは媒体作成中の暗証データの盗難リスクなども回避されるようになる。

【００１４】請求項２の構成は、さらに両照合用データの生成に当たり、他人の者との一致を排除する構成である。すなわち、暗証データは、通常ユーザ側が自由に選択・決定するため、ユーザ間で同じものを選択してしまう確率は全くないとは言えず、従って照合用データも個々のユーザにユニークなものになるとは限らない。そこで、ユーザ側に選択権のない（或いはユーザ側の選択権が限られる）、各ユーザ毎にユニークな状態で割り当てられるユーザＩＤなどのユーザデータを照合用データの生成に利用することにした。

【００１５】具体的には、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、コンピュータ上に第１の照合用データ及びユーザデータが読み取られると共に、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第２の照合用データが算出され、該第２の照合用データと前記第１の照合用データとが照合されることで、本人確認が行われることを特徴としている。

【００１６】上記ユーザデータと暗証データは、一方を他方の後に一連につなげて使用する場合の他、両データを互いに加減乗除して使用したり、或いは適当な数字で加減乗除しその後一連につなげて使用したりするなど、両データを使用することで、照合用データの生成前にユニークなデータとして得られるものであれば、これらのデータの用いられ方には、特に限定はない。

【００１７】上記請求項１、請求項２の構成において、使用される媒体に記録されているものは、第１の照合用データであり、上述のように解析することはできないが、暗証データが盗用された場合は、上記媒体乃至そのコピー品を使用する限り、本人と誤認識されてしまう可能性がある。そのようなことを想定した場合、該媒体に記載される暗証データは、外部から感知できるユーザの特徴を何らかの形で検出し、任意のデータに変換したものを用いる方が良い。すなわち、ユーザに記憶されるものではなく、例えばユーザの身体的特徴（指紋、眼球の光彩部分の特徴、腕等に浮き出ている血管の位置情報）を検出し、その検出データを使用すれば、ユーザは暗証データを覚える必要が無くなって、単に検出機器にその身体部分を検出させれば良く、そのために他人による暗証データの盗用はできなくなるため、セキュリティレベルは非常に高度のものとなる（ハッキングによるなりすましは不可能となる）。これは、以下に示す他の請求項についても同様である（請求項３、６、９、１２、１５、１８及び２３）。

【００１８】請求項４の構成は、上記請求項１の本人確認方法の構成を、本人確認を行う装置の構成として捉え直して規定したものであり、より具体的な構成としては、少なくとも暗証データに対して一方向性関数により処理して得られる第１の照合用データの記録された媒体から、第１の照合用データを読み取る照合用データ読み取り手段と、暗証データの入力手段と、入力された暗証データに対して上記と同じ一方向性関数によって第２の照合用データを算出する算出手段と、上記第２の照合用データと前記第１の照合用データとを照合する照合手段と、上記照合結果に基づき、本人か否かの判定を行う判定手段とを有することを特徴としている。

【００１９】請求項７の構成は、上記本人確認装置で使用される媒体の作成装置を規定するものであり、具体的には、少なくとも暗証データが与えられることにより一方向性関数により処理して第１の照合用データを算出する演算手段と、該第１の照合用データを媒体に書き込む照合用データ書き込み手段とを有することを特徴としている。

【００２０】請求項１０の構成は、上記請求項１の方法乃至請求項４の装置で使用可能な媒体の構成を規定したものであり、より具体的には、暗証データに対して一方向性関数により処理して得られる第１の照合用データを格納するための領域を有する媒体である。なお、このような媒体としては、磁気記録カード、ＩＣカード、光磁気カードなどがあり、データを記録できるものであれば、記録形式、媒体形状などの如何に拘わらず、用いることができる。

【００２１】請求項５の構成は、上記請求項２の本人確認方法の構成を、本人確認を行う装置の構成として捉え直して規定したものであり、より具体的な構成としては、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、第１の照合用データ及びユーザデータを読み取る照合用データ読み取り手段と、暗証データの入力手段と、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第２の照合用データを算出する算出手段と、上記第２の照合用データと前記第１の照合用データとを照合する照合手段と、上記照合結果に基づき、本人か否かの判定を行う判定手段とを有することを特徴としている。

【００２２】請求項８の構成は、上記本人確認装置で使用される媒体の作成装置を規定するものであり、具体的には、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列が与えられることにより一方向性関数により処理して第１の照合用データを算出する演算手段と、該第１の照合用データを媒体に書き込む照

合用データ書き込み手段とを有することを特徴としている。

【００２３】請求項１１の構成は、上記請求項２の方法乃至請求項５の装置で使用可能な媒体の構成を規定したものであり、より具体的には、ユニークなユーザデータと暗証データを構成要素とするデータ列に対して一方向性関数により処理して得られる第１の照合用データを格納するための領域を有する媒体である。

【００２４】一方請求項１３の構成は、上記本人確認がなされた際、媒体中にユーザが任意の情報を記録する（保管情報の記録）と共に、それ以後、この保管情報の記録された媒体から、該保管情報を取り出して利用しようとする場合に、その利用をしようとする者が媒体の正しい所有者又は媒体に上記保管情報を記録した者であることの照合と記録された保管情報に改竄がないことの確認が行えるようにする構成を提供せんとするものである。

【００２５】すなわち、請求項１３に係る媒体保管情報の処理方法の構成は、少なくとも暗証データに対して第１の一方向性関数により処理して得られる第１の照合用データの記録された媒体から、第１の照合用データが読み取られ、入力された暗証データに対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致したことにより、該保管情報と第３の照合用データとが記録されたという経緯を有する上記媒体から、コンピュータ上に第１の照合用データ、第３の照合用データ及び上記保管情報が読み取られるステップと、別途入力された暗証データに対し上記第１の一方向性関数によって第４の照合用データが算出されるステップと、第４の照合用データと読み取られた前記第１の照合用データとが照合されるステップと、読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データが算出されるステップと、上記照合ステップで第４の照合用データと第１の照合用データとが一致したことを条件として、読み取られた前記第３の照合用データと上記第５の照合用データとが照合されるステップと、第３の照合用データと第５の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行することを特徴としている。

【００２６】上記構成では、ユーザ側で任意の保管情報（例えばユーザの作成したソフトウェアやマクロ、機器操作情報、個人取引情報振込カード情報など）が記録された媒体が対象とされる。そのため、ユーザ側で保管情報の記録操作を、下記のようにして行うことになる。

【００２７】まず、ユーザは、少なくとも暗証データに対して第１の一方向性関数により処理して得られる第１の照合用データの記録された媒体を提供し、そこから、コンピュータ上に第１の照合用データを読み取らせる。一方ユーザは、コンピュータから暗証データの入力を要求され、これを入力する。ユーザがこれを入力した場合、該暗証データに対して上記第１の一方向性関数によって第２の照合用データが算出され、第２の照合用データと前記第１の照合用データとが照合される。他方入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出される。そして、第２の照合用データと第１の照合用データとの照合でこれらのデータが一致した場合、前記保管情報と第３の照合用データとが、コンピュータによって、上記媒体に記録される。

【００２８】すなわち、保管情報の媒体への記録に当たって、第１の照合用データと第２の照合用データとが照合されることで、本人確認を行い、媒体の正しい所有者のみが、媒体に上記保管情報の記録を行えることになる。

【００２９】このような媒体から上記保管情報を読み出して、該保管情報の処理を行う場合にも、次のようにして、記録された保管情報の利用者が、媒体の正しい所有者乃至該媒体への保管情報記録者であるという照合と、記録された保管情報に改竄がないことの確認を行うことになる。

【００３０】まず、ユーザは上記媒体を提供し、該媒体から、他のコンピュータ上に第１の照合用データ、第３の照合用データ及び上記保管情報を読み取らせる。またユーザは別途暗証データの入力を要求されるが、これに呼応して暗証データの入力を該コンピュータに対して行うと、該暗証データに対し上記第１の一方向性関数によって第４の照合用データが算出され、第４の照合用データと読み取られた前記第１の照合用データとが照合される。他方読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データが算出される。そして上記照合の結果、第４の照合用データと第１の照合用データとが一致した場合（記録された保管情報の利用者が、媒体の正しい所有者乃至該媒体への保管情報記録者であるという本人確認がされた場合）、読み取られた前記第３の照合用データと上記第５の照合用データとが照合される。第３の照合用データと第５の照合用データとが一致する場合は、保管情報の改竄がないと判断でき、読み取られた保管情報を、該コンピュータ上で処理することになる。

【００３１】請求項１６の構成は、上記媒体保管情報の処理方法で使用される媒体について規定しており、具体

的には、少なくとも暗証データに対して第１の一方向性関数により処理して得られる第１の照合用データを格納するための第１の格納領域と、該格納領域に第１の照合用データの記録された状態から、該照合用データが読み取られ、入力された暗証データに対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致した場合に格納される、該保管情報ための第２の格納領域と第３の照合用データのための第３の格納領域とを有する媒体である。

【００３２】請求項１４の構成は、請求項２と同様、照合用データの生成に当たり、他人の者との一致を排除する構成である。すなわち、暗証データの他に、各ユーザ毎にユニークな状態で割り当てられるユーザデータも照合用データの生成に利用する。より具体的な構成としては、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第１の一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、第１の照合用データ及びユーザデータが読み取られ、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致したことにより、該保管情報と第３の照合用データとが記録されたという経緯を有する上記媒体から、コンピュータ上にユーザデータ、第１の照合用データ、第３の照合用データ及び上記保管情報が読み取られるステップと、別途入力された暗証データ及び読み取られた上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第４の照合用データが算出されるステップと、第４の照合用データと読み取られた前記第１の照合用データとが照合されるステップと、読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データが算出されるステップと、上記照合ステップで第４の照合用データと第１の照合用データとが一致したことを条件として、読み取られた前記第３の照合用データと上記第５の照合用データとが照合されるステップと、第３の照合用データと第５の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行することを特徴としている。

【００３３】請求項１７の構成は、上記媒体保管情報の処理方法で使用される媒体について規定しており、具体的には、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第１の一方向性関数により処理して得られる第１の照合用データを格納するための第１の格納領域と、上記ユーザデータを格納するための第２の格納領域と、これらの格納領域に第１の照合用データ及びユーザデータの記録された状態から、第１の照合用データ及びユーザデータが読み取られ、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致した場合に格納される、該保管情報ための第３の格納領域と第３の照合用データのための第４の格納領域とを有する媒体である。

【００３４】請求項１９～請求項２２までの構成は、請求項１及び請求項２に記載の構成並びに請求項１３及び請求項１４に記載の構成を、コンピュータで実行させるための、該コンピュータで実行可能なプログラムを規定している。すなわち、上述した課題を解決するための構成として、上記各ステップを、コンピュータの構成を利用することで実行する、該コンピュータで読み込まれて実行可能なプログラムを開示する。この場合、コンピュータとは中央演算処理装置の構成を含んだ汎用的なコンピュータの構成の他、特定の処理に向けられた専用機などを含むものであっても良く、中央演算処理装置の構成を伴うものであれば特に限定はない。

【００３５】コンピュータに上記各ステップを実行させるための以下に示すプログラムが該コンピュータに読み出されて実行されると、請求項１及び請求項２に記載の構成並びに請求項１３及び請求項１４の構成に規定された各ステップと同様なステップが実行されることになる。

【００３６】上記プログラムは、それ自身使用の対象となる他、後述のように記録媒体に記録されて配布乃至販売され、また通信などにより送信されて、譲渡の対象とすることもできるようになる。

【００３７】尚、請求項１９～請求項２２記載の各ステップのうち一部の機能は、コンピュータに組み込まれた機能（コンピュータにハードウェア的に組み込まれている機能でも良く、該コンピュータに組み込まれているオ

ペレーティングシステムや他のアプリケーションプログラムなどによって実現される機能でも良い）によって実現され、前記プログラムには、該コンピュータによって達成されるこれらの機能を呼び出すあるいはリンクさせる命令が含まれるだけの構成であったとしても、本発明に規定する構成に含まれることは言うまでもない。

【００３８】これは、請求項１及び請求項２に記載の構成並びに請求項１３及び請求項１４の構成に規定された各ステップの一部が、例えばオペレーティングシステムなどによって達成される機能の一部で代行され、上記プログラムにはその機能を実現するためのモジュールなどが直接記録されているわけではないが、それらの機能を達成するオペレーティングシステムの機能の一部を、呼び出したりリンクさせるようにしてあれば、実質的に同じ構成となるからである。

【００３９】またこれらのプログラムが記録媒体に固定される（請求項２４）ことで、これをソフトウェア商品として容易に配布、販売することができるようになる。また、既存のハードウェア資源を用いて該プログラムを使用することにより、既存のハードウェアで新たなアプリケーションとしての本発明の構成が容易に実行できるようになる。また該プログラムを固定する記録媒体の構成は、上記のソフトウェア商品として配布・販売する構成の他、ＲＡＭやＲＯＭなどの内部記憶装置の構成やハードディスクなどの外部記憶装置の構成も、そのようなプログラムがそこに記録されれば、該記録媒体に含まれることは言うまでもない。

【００４０】そのうち、請求項１９のプログラムの構成は、請求項１の構成に対応する構成であり、その具体的構成は、コンピュータに、少なくとも暗証データに対して一方向性関数により処理して得られる第１の照合用データの記録された媒体から、第１の照合用データを読み取らせるステップと、入力された暗証データに対し上記と同じ一方向性関数によって第２の照合用データを算出させるステップと、該第２の照合用データと前記第１の照合用データとを照合させ、本人確認を行うステップとを実行させることを特徴としている。

【００４１】請求項２０のプログラムの構成は、請求項２の構成に対応する構成であり、その具体的構成は、コンピュータに、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、第１の照合用データ及びユーザデータを読み取らせるステップと、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第２の照合用データを算出させるステップと、該第２の照合用データと前記第１の照合用データとを照合させ、本人確認を行うステップとを実行させることを特徴としている。

【００４２】請求項２１のプログラムの構成は、請求項１３の構成に対応する構成であり、その具体的構成は、コンピュータに、少なくとも暗証データに対して第１の一方向性関数により処理して得られる第１の照合用データの記録された媒体から、第１の照合用データが読み取られ、入力された暗証データに対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致したことにより、該保管情報と第３の照合用データとが記録されたという経緯を有する上記記体から、第１の照合用データ、第３の照合用データ及び上記保管情報を読み取らせるステップと、別途入力された暗証データに対し上記第１の一方向性関数によって第４の照合用データを算出させるステップと、第４の照合用データと読み取られた前記第１の照合用データとを照合させるステップと、読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データを算出させるステップと、上記照合ステップで第４の照合用データと第１の照合用データとが一致したことを条件として、読み取られた前記第３の照合用データと上記第５の照合用データとを照合させるステップと、第３の照合用データと第５の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行させることを特徴としている。

【００４３】請求項２２のプログラムの構成は、請求項１４の構成に対応する構成であり、その具体的構成は、コンピュータに、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第１の一方向性関数により処理して得られる第１の照合用データ及び上記ユーザデータの記録された媒体から、第１の照合用データ及びユーザデータが読み取られ、入力された暗証データ及び上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第２の照合用データが算出された後、第２の照合用データと前記第１の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第３の照合用データが算出され、第２の照合用データと第１の照合用データとが一致したことにより、該保管情報と第３の照合用データとが記録されたという経緯を有する上記媒体から、ユーザデータ、第１の照合用データ、第３の照合用データ及び上記保管情報を読み取らせるステップと、別途入力された暗証データ及び読み取られた上

記ユーザデータを少なくとも構成要素とするデータ列に対し上記第１の一方向性関数によって第４の照合用データを算出させるステップと、第４の照合用データと読み取られた前記第１の照合用データとを照合させるステップと、読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第１の一方向性関数又は第２の一方向性関数によって第５の照合用データを算出させるステップと、上記照合ステップで第４の照合用データと第１の照合用データとが一致したことを条件として、読み取られた前記第３の照合用データと上記第５の照合用データとを照合させるステップと、第３の照合用データと第５の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行させることを特徴としている。

【００４４】請求項２４の構成は、上記請求項１９～請求項２３のいずれかのプログラムを記録したコンピュータ読み取り可能な記録媒体について規定する。

【００４５】

【発明の実施の形態】以下、本発明の実施の形態を図示例と共に説明する。

（実施例１）図１は、本発明によって、ＩＣカードよりなる媒体１の所有者が本人であることの確認が行えるシステムを、金融機関のＡＴＭ（Automatic Tellar Machine）において適用した場合の、媒体作成装置２による媒体作成工程を示す説明図である。

【００４６】同図に示すように、ユーザは、カード発行側に対し、ＩＣカード（媒体１）の発行して欲しい旨の申込を行うと、カード発行側は、該ユーザ用にユニークなユーザＩＤを割り当て、それをユーザ側に通知する。またカード発行側は、該ユーザに対して、該ユーザが望む暗証番号を入力するよう求め、ユーザ側からの暗証番号の通知を受け付ける。以上の工程は、ユーザ側がネットを介してカード発行側のサーバにアクセスすることで行われるが、ネットを使わず、窓口において行っても良い。

【００４７】尚、上記暗証番号は、ユーザが望む適宜の数字・文字・記号などではなく、たとえば指紋、眼球の光彩部分の特徴、腕等に浮き出ている血管の位置情報などのユーザの身体的特徴を検出させて、その検出データを用いるようにしても良い。媒体１に記録される第１の照合用データは、後述するように、ハッシュ関数で処理されて得られるものであるため、解析することはできないが、暗証番号が盗用された場合は、上記媒体１乃至そのコピー品を使用する限り、本人と誤認識されてしまう可能性がある。従って、そのような盗用ができないように、該媒体１に記載される暗証番号は、ユーザの身体的特徴の検出データなどの方、他人のハッキングによるなりすましを防ぐ意味で望ましい。

【００４８】ここで、媒体作成に必要なユーザＩＤと暗証番号が揃うので、これらが、後述する媒体作成装置２に入力される。該媒体作成装置２は、これらの入力データに対して、ハッシュ関数処理を行い、第１の照合用データを生成する。そして該第１の照合用データを、上記ユーザＩＤと共に、前記媒体１に書き込む。この媒体１は、上記ユーザに交付される。

【００４９】図２は、上記媒体作成装置２の機能構成を示す機能ブロック図である。同図に示すように、ユーザＩＤと暗証番号のデータ列が与えられることによりハッシュ関数で処理して第１の照合用データを算出する演算手段２１と、該第１の照合用データを媒体１に書き込む書込手段２２とを有している。

【００５０】このような構成により本人確認用に上記媒体１が作成されるので、できあがった媒体１には、ユーザＩＤと第１の照合用データが記録されるのみで、暗証番号そのものはない。しかも第１の照合用データは、逆方向の解析が不能な（一方向性の）ハッシュ関数で処理されており、該第１の照合用データからは、暗証番号などを割り出すことはできない。さらに元となったデータには、ユーザＩＤが含まれており、それ自身はユニークなデータであるため、生成された第１の照合用データもユニークなものとなり、他人のものと同一になることはない。

【００５１】図３は、ユーザが上記媒体１を使用して、本人確認を行う場合に使用される本人確認装置３における本人確認処理の工程説明図である。この場合の本人確認装置３は、金融機関における上記ＡＴＭで構成されることになる。

【００５２】同図に示すように、ユーザは、本人確認装置３の挿入口に上記媒体１を挿入する。すると暗証番号の入力が求められるので、暗証番号の入力を行う。ここでは、媒体１の作成時の状態に応じて、ユーザの身体的特徴をセンサなどで検出させ、その検出データを暗証番号として入力することもできる。

【００５３】ここで、本人確認の際に第２の照合用データ生成に必要なユーザＩＤ（媒体１より読み込まれる）と暗証番号（ユーザによる入力）が揃うので、これらのデータに対して、上記と同一のハッシュ関数を用いた処理が行われ、第２の照合用データが生成される。そして媒体１より読み込まれた第１の照合用データと生成された該第２の照合用データとの照合が行われる。これらのデータが一致すれば、媒体１の所有者が該ユーザであると確認され（本人確認がなされ）、該本人確認装置３が組み込まれているＡＴＭにおけるその他の操作が許可され、以後ユーザによって、ＡＴＭにおける任意の操作が実施される。

【００５４】図４は、上記本人確認装置３の機能構成を示す機能ブロック図である。同図に示すように、上記媒体１から、第１の照合用データ及びユーザＩＤを読み取る照合用データ読み取り手段３１と、テンキーやタッチパネル（或いはユーザの身体的特徴を検出するセンサ）

などで構成される暗証番号の入力手段３２と、読み取られたユーザＩＤと入力された暗証番号のデータ列に対し上記と同じハッシュ関数によって第２の照合用データを算出する算出手段３３と、生成された第２の照合用データと読み取られた第１の照合用データとを照合する照合手段３４と、照合結果に基づき、本人か否かの判定を行う判定手段３５とを有している。

【００５５】上記構成によれば、媒体１からは上述のように、暗証番号の割り出しはできないので、本人確認を行う際に、媒体１の所持人に対し、入力手段３２からの暗証番号の入力を要求し、入力された暗証番号及び読み取られたユーザＩＤに対して、算出手段３３により上記と同一のハッシュ関数で処理し、その結果得られた第２の照合用データと、前記媒体１より読み取られた第１の照合用データとが、照合手段３４で突き合わされ、判定手段３５により、本人確認が行われるので、他の装置との接続が要求されることなく媒体１単体で、媒体１の所持人が、ユーザ本人であると確認することができるようになる。しかも媒体１に格納されるデータは、上述のように、本人確認のために入力されるべき暗証番号そのものなどのデータではなく、しかも媒体１上に格納されるデータからは、入力の要求される暗証番号の割り出しが困難なため、セキュリティも向上することになる。

【００５６】図５は、上記媒体作成装置２における処理の手順を示すフローチャートである。同図に示すように、ユーザ側からのアクセスで、媒体１の発行の申込があると、該媒体作成装置２により、該ユーザに対するユーザＩＤが決定され、該ユーザＩＤが、このユーザに通知される（ステップＳ１０１）。そして通知済か否かの確認がなされ（ステップＳ１０２）、通知していなければ（ステップＳ１０２；Ｎｏ）、ステップＳ１０１に復帰する。

【００５７】通知済であれば（ステップＳ１０２；Ｙｅｓ）、ユーザの希望する暗証番号の入力（ユーザの身体的特徴を検出させる場合もある）を促す表示がなされ（ステップＳ１０３）、暗証番号が入力されたか否かがチェックされる（ステップＳ１０４）。該暗証番号の入力がなければ（ステップＳ１０４；Ｎｏ）、前記ステップＳ１０３に復帰する。

【００５８】上記ユーザＩＤと入力された暗証番号を基にハッシュ関数処理がなされ、第１の照合用データが生成される（ステップＳ１０５）。

【００５９】生成された第１の照合用データが存在するかがチェックされ（ステップＳ１０６）、該データがなければ（ステップＳ１０６；Ｎｏ）、前記ステップＳ１０５に復帰する。

【００６０】上記第１の照合用データが確認されれば（ステップＳ１０６；Ｙｅｓ）、媒体１に当該データ及びユーザＩＤの書き込みがなされる（ステップＳ１０７）。そして該媒体１上に第１の照合用データ及びユーザＩＤがあるか否かが確認される（ステップＳ１０８）。

【００６１】媒体１上に第１の照合用データ及びユーザＩＤが無ければ（ステップＳ１０８；Ｎｏ）、前記ステップＳ１０７に復帰する。反対に媒体１上にこれらのデータがあれば（ステップＳ１０８；Ｙｅｓ）、処理を終了する。そしてこの媒体１がユーザに交付される。

【００６２】図６は、上記本人確認装置３における処理の手順を示すフローチャートである。同図に示すように、ＡＴＭ上の本人確認装置３では、挿入口における媒体１の挿入が検出され（ステップＳ２０１）、該媒体１が挿入されたか否かがチェックされる（ステップＳ２０２）。媒体１の挿入が検出されない場合（ステップＳ２０２；Ｎｏ）、前記ステップＳ２０１に戻る。

【００６３】媒体１の挿入が検出されれば（ステップＳ２０２；Ｙｅｓ）、該媒体１からのユーザＩＤ及び第１の照合用データの読み取りがなされる（ステップＳ２０３）。そしてこれらのデータが読み取られたか否かがチェックされる（ステップＳ２０４）。読み取りが完了していなければ（ステップＳ２０４；Ｎｏ）、前記ステップＳ２０１に復帰する。

【００６４】上記データの読み取りが完了していれば（ステップＳ２０４；Ｙｅｓ）、ユーザの暗証番号の入力（ユーザの身体的特徴を検出させる場合もある）を促す表示がなされ（ステップＳ２０５）、暗証番号が入力されたか否かがチェックされる（ステップＳ２０６）。該暗証番号の入力がなければ（ステップＳ２０６；Ｎｏ）、前記ステップＳ２０５に戻る。

【００６５】上記暗証番号の入力があった場合（ステップＳ２０６；Ｙｅｓ）、読み取られた上記ユーザＩＤと入力された暗証番号を基にハッシュ関数処理がなされ、第２の照合用データが生成される（ステップＳ２０７）。

【００６６】生成された第２の照合用データが存在するかがチェックされ（ステップＳ２０８）、該データがなければ（ステップＳ２０８；Ｎｏ）、前記ステップＳ２０７に復帰する。

【００６７】上記第２の照合用データが確認されれば（ステップＳ２０８；Ｙｅｓ）、両照合用データの照合がなされる（ステップＳ２０９）。その照合結果で、両データが一致するか否かがチェックされ（ステップＳ２１０）、一致しなければ（ステップＳ２１０；Ｎｏ）、前記ステップＳ２０５に復帰する。

【００６８】反対に両データが一致する場合（ステップＳ２１０；Ｙｅｓ）、本人確認ができたとして（ステップＳ２１１）、該本人確認装置３における処理は終了し、入出金処理、振込・振り替え処理、照会処理など、種々の前記ＡＴＭにおける操作が可能になる。

【００６９】上記実施例構成によれば、媒体１中に格納されるデータは、暗証番号そのものではなく、ハッシュ

関数により処理して得られる第１の照合用データであり、そのため、仮に媒体１からこれらのデータが読み出せたとして、第１の照合用データからは、暗証番号を割り出すことはできない。従って本人確認の際に暗証番号の入力（場合によりユーザの身体的特徴の検出）を要求することで、入力された暗証番号に対し上記と同一のハッシュ関数で処理し、その結果得られた第２の照合用データと、前記媒体１より読み取った第１の照合用データとの突き合わせを行い、その照合結果で本人確認処理を行えば、他の装置との接続が要求されることなく、該媒体１だけで本人確認が完結できることになる。また媒体１上に格納されるデータは、本人確認のために入力される暗証番号そのものではなく、しかも媒体１上に格納されるデータからは、上記入力の要求される暗証番号の割り出しが困難なため、セキュリティも向上することになる。すなわち、ユーザ以外は、いかなる者も真の暗証番号を目にすることなく安全に媒体１が作成され、媒体１の盗難、偽造などに対しても、極めて強力に対抗できるセキュリティを提供することができるようになり、さらに郵送中や媒体発行者の業務遂行中、或いは媒体１作成中の暗証番号の盗難リスクなども回避されるようになる。

【００７０】（実施例２）図７～図１２は、本発明によって、ＩＣカードよりなる媒体１の所有者が、例えば金融機関のＡＴＭに備えられた後述する保管情報処理装置５において実行される処理シーケンスや該装置５において実行できるソフトウェアなどの自己の希望する情報を予め該媒体１に登録しておき、該保管情報処理装置５で上記所有者がユーザ本人であると確認された際に、それらの情報の処理が行われるシステムを説明したものであり、そのうち特に図７は、媒体作成装置２による媒体作成工程を示す説明図である。

【００７１】実施例１と同様、ユーザは、カード発行側に対し、ＩＣカード（媒体１）の発行して欲しい旨の申込を行うと、カード発行側は、該ユーザ用にユニークなユーザＩＤを割り当て、それをユーザ側に通知する。またカード発行側は、該ユーザに対して、該ユーザが望む暗証番号を入力するよう求め、ユーザ側からの暗証番号の通知を受け付ける。以上の工程は、ユーザ側がネットを介してカード発行側のサーバにアクセスすることで行われるが、ネットを使わず、窓口において行っても良い。

【００７２】また、本実施例構成においても、上記暗証番号は、ユーザが望む適宜の数字・文字・記号などではなく、たとえば指紋、眼球の光彩部分の特徴、腕等に浮き出ている血管の位置情報などのユーザの身体的特徴を検出させて、その検出データを用いるようにしても良い。

【００７３】ここで、媒体作成に必要なユーザＩＤと暗証番号が揃うので、これらが、媒体作成装置２に入力される。該媒体作成装置２は、これらの入力データに対して、第１のハッシュ関数を用いた処理を行い、第１の照合用データを生成する。そして該第１の照合用データを、上記ユーザＩＤと共に、前記媒体１に書き込む。この媒体１は、上記ユーザに交付される。

【００７４】上記媒体作成装置２は、前記実施例１の構成と同じであるので、ここではその説明は省略する。

【００７５】このような構成により本人確認用に上記媒体１が作成されるので、できあがった媒体１には、ユーザＩＤと第１の照合用データが記録されるのみで、暗証番号そのものはない。しかも第１の照合用データは、逆方向の解析が不能な第１のハッシュ関数で処理されており、該第１の照合用データからは、暗証番号などを割り出すことはできない。さらに元となったデータには、ユーザＩＤが含まれており、それ自身はユニークなデータであるため、生成された第１の照合用データもユニークなものとなり、他人のものと同一になることはない。

【００７６】図８は、後述する保管情報処理装置５において実行される処理シーケンスや該装置５において実行できるソフトウェアなどのユーザ自身が望む情報を、交付された媒体１に、予め登録しておくための情報保管装置４の構成説明図である。

【００７７】該情報保管装置４は、前記図７で示したように、カード発行側から貸与された情報保管ソフトウェアのインストールされたユーザ側のパソコンと、媒体１の情報を読み書きするために該パソコンに接続されたカードリーダライタからなるデータ読取書込手段４１とで構成されている。尚、上記情報保管ソフトウェア中に規定される第１のハッシュ関数（第１の算出手段４３で使用）は、上記媒体作成装置２及び後述する保管情報処理装置５において夫々第１の照合用データ及び第４の照合用データ生成時に使用されるハッシュ関数と同一のものであり、また同じく上記情報保管ソフトウェア中に規定される第２のハッシュ関数（第２の算出手段４６で使用）は、保管情報処理装置５において第５の照合用データ生成時に使用されるハッシュ関数と同一のものである。

【００７８】ユーザは、この情報保管装置４を使用して、自分の望む情報を、交付された媒体１に予め登録しておくことができるようになる。ここで登録しておくことのできる情報とは、上述のように、後述する保管情報処理装置５（本実施例では、特定カード向けに該カード上にユーザの規定する処理の実行ができるようにした、ＪＡＶＡ、ＭＵＬＴＯＳ、ＷＩＮＤＯＷＳなどの汎用ＯＳの稼働するＡＴＭ）で実行することが予定される複数処理の連続実行シーケンスや該装置５において実行できるソフトウェアなどがある。

【００７９】図９は、上記情報保管装置４の機能構成を示す機能ブロック図である。同図に示すように、上記媒体１から、第１の照合用データ及びユーザＩＤを読み取

り、後に、算出手段４６によって算出された第３の照合用データ及び保管情報を媒体１に書き込むことができるデータ読取書込手段４１と、テンキーやタッチパネル（或いはユーザの身体的特徴を検出するセンサ）などで構成される暗証番号の入力手段４２と、読み取られたユーザＩＤと入力された暗証番号のデータ列に対して、媒体作成装置２と同じ第１のハッシュ関数によって第２の照合用データを算出する第１の算出手段４３と、生成された第２の照合用データと読み取られた第１の照合用データとを照合する照合手段４４と、照合結果に基づき、本人か否かの判定を行う判定手段４５と、本人であると判定された場合に、ユーザのパソコン内の記憶装置（ハードディスクなど）に記録された或いはキーボードなどから入力される上記保管情報と入力された上記暗証番号を基に、第２のハッシュ関数によって第３の照合用データを算出する第２の算出手段４６とを有している。

【００８０】上記情報保管装置４は、ユーザがパソコン上で情報保管ソフトウェアを起動させることで構成される。そして、ユーザが、ユーザＩＤ及び第１の照合用データの記録された上記媒体１をデータ読取書込手段４１に挿入し、該媒体１から、ユーザＩＤ及び第１の照合用データを読み取らせる。すると、暗証番号の入力が求められるので、ユーザはこれを入力する（又はセンサに身体的特徴を検出させる）。入力（又は検出）された暗証番号と読み取られたユーザＩＤを基に、第１の算出手段４３により、第１のハッシュ関数を使用した処理がなされ、第２の照合用データが生成される。生成された第２の照合用データと読み取られた前記第１の照合用データとが、照合手段４４により照合される。その照合結果が判定手段４５で判定され、両データが一致すれば、該媒体１の所有者がユーザであると判定される。そして上記記憶装置或いはキーボードなどから入力された上記保管情報と入力（又は検出）された前記暗証番号とからなるデータ列を基に、第２の算出手段４６により、第２のハッシュ関数を用いた処理がなされ、第３の照合用データが生成される。生成された第３の照合用データと前記保管情報とが、前記データ読取書込手段４１により、媒体１に書き込まれる。

【００８１】図１０は、上記保管情報処理装置５の機能構成を示す機能ブロック図である。同図に示すように、保管情報処理装置５の構成は、上記媒体１から、ユーザＩＤ、第１の照合用データ、第３の照合用データ及び上記保管情報を読み取るデータ読み取り手段５１と、テンキーやタッチパネル（或いはユーザの身体的特徴を検出するセンサ）などで構成される暗証番号の入力手段５２と、読み取られたユーザＩＤと入力された暗証番号のデータ列に対して、媒体作成装置２及び情報保管装置４と同じ第１のハッシュ関数によって第４の照合用データを算出する第１の算出手段５３と、生成された第４の照合用データと読み取られた第１の照合用データとを照合する第１の照合手段５４と、照合結果に基づき、本人か否かの判定を行う第１の判定手段５５と、その媒体所有者が本人であると判定された場合に、読み取られた保管情報と入力された暗証番号のデータ列に対して、前記情報保管装置４と同じ第２のハッシュ関数によって第５の照合用データを算出する第２の算出手段５６と、生成された第５の照合用データと読み取られた第３の照合用データとを照合する第２の照合手段５７と、照合結果に基づき、保管情報の内容に改竄がないか否かの判定を行う第２の判定手段５８と、保管情報の内容に改竄がないと判定された場合に、保管情報の処理を行う処理手段５９とを有している。

【００８２】図１１は、上記のようにしてユーザに保管情報の書き込みが行われた媒体１を使用して、該ユーザが、金融機関のＡＴＭ上で当該保管情報を実行させることを可能にする保管情報処理装置５における処理の工程説明図である。この場合の保管情報処理装置５は、金融機関における上記ＡＴＭで構成されることになる。

【００８３】同図に示すように、ユーザは、保管情報処理装置５の挿入口に上記媒体１を挿入する。すると暗証番号の入力が求められるので、暗証番号の入力を行う。ここでは、媒体１の作成時の状態に応じて、ユーザの身体的特徴をセンサなどで検出させ、その検出データを暗証番号として入力することもできる。

【００８４】ここで、本人確認の際に第４の照合用データ生成に必要なユーザＩＤ（媒体１より読み込まれる）と暗証番号（ユーザによる入力）が揃うので、これらのデータに対して、上記と同一の第１のハッシュ関数を用いた処理が行われ、第４の照合用データが生成される。そして媒体１より読み込まれた第１の照合用データと生成された該第４の照合用データとの照合が行われる。これらのデータが一致すれば、媒体１の所有者が該ユーザであると確認される（本人確認がなされる）。

【００８５】本人確認がなされると、読み出された保管情報と入力された前記暗証番号に対して、情報保管装置４で用いられたと同一の第２のハッシュ関数を用いた処理が行われ、第５の照合用データが生成される。そして媒体１より読み込まれた第３の照合用データと生成された該第５の照合用データとの照合が行われる。これらのデータが一致すれば、媒体１に保管されている情報には改竄がないと判断される（不正アクセスがないと判断される）。その後上記ＡＴＭ上で、該保管情報の処理がなされる。

【００８６】図１２は、上記保管情報処理装置５における処理の手順を示すフローチャートである。同図に示すように、ＡＴＭ上の保管情報処理装置５では、挿入口における媒体１の挿入が検出され（ステップＳ３０１）、該媒体１が挿入されたか否かがチェックされる（ステップＳ３０２）。媒体１の挿入が検出されない場合（ステップＳ３０２；Ｎｏ）、前記ステップＳ３０１に戻る。

【００８７】媒体１の挿入が検出されれば（ステップＳ３０２；Ｙｅｓ）、該媒体１からのユーザＩＤ、第１及び第３の照合用データ並びに保管情報の読み取りがなされる（ステップＳ３０３）。そしてこれらのデータが読み取られたか否かがチェックされる（ステップＳ３０４）。読み取りが完了していなければ（ステップＳ３０４；Ｎｏ）、前記ステップＳ３０１に復帰する。

【００８８】上記データの読み取りが完了していれば（ステップＳ３０４；Ｙｅｓ）、ユーザの暗証番号の入力（ユーザの身体的特徴を検出させる場合もある）を促す表示がなされ（ステップＳ３０５）、暗証番号が入力されたか否かがチェックされる（ステップＳ３０６）。該暗証番号の入力がなければ（ステップＳ３０６；Ｎｏ）、前記ステップＳ３０５に戻る。

【００８９】上記暗証番号の入力があった場合（ステップＳ３０６；Ｙｅｓ）、読み取られた上記ユーザＩＤと入力された暗証番号を基に第１のハッシュ関数による処理がなされ、第４の照合用データが生成される（ステップＳ３０７）。

【００９０】生成された第４の照合用データが存在するかがチェックされ（ステップＳ３０８）、該データがなければ（ステップＳ３０８；Ｎｏ）、前記ステップＳ３０７に復帰する。

【００９１】上記第４の照合用データが確認されれば（ステップＳ３０８；Ｙｅｓ）、読み取られた第１の照合用データと生成された第４の照合用データとの照合がなされる（ステップＳ３０９）。その照合結果で、両データが一致するか否かがチェックされ（ステップＳ３１０）、一致しなければ（ステップＳ３１０；Ｎｏ）、前記ステップＳ３０５に復帰する。

【００９２】反対に両データが一致する場合（ステップＳ３１０；Ｙｅｓ）、本人確認ができたとして、読み取られた保管情報と入力された暗証番号を基に第２のハッシュ関数による処理がなされ、第５の照合用データが生成される（ステップＳ３１１）。

【００９３】生成された第５の照合用データが存在するかがチェックされ（ステップＳ３１２）、該データがなければ（ステップＳ３１２；Ｎｏ）、前記ステップＳ３１１に復帰する。

【００９４】上記第５の照合用データが確認されれば（ステップＳ３１２；Ｙｅｓ）、読み取られた第３の照合用データと生成された第５の照合用データとの照合がなされる（ステップＳ３１３）。その照合結果で、両データが一致するか否かがチェックされ（ステップＳ３１４）、一致しなければ（ステップＳ３１４；Ｎｏ）、保管情報の処理がなされない旨表示し、該処理を拒否する（ステップＳ３１６）。

【００９５】反対に両データが一致する場合（ステップＳ３１４；Ｙｅｓ）、上記保管情報に従った処理（その保管情報の内容に応じた入出金処理、振込・振り替え処理、照会処理などの処理）が、該ＡＴＭ上で実行される（ステップＳ３１５）。

【００９６】上記実施例構成によれば、媒体１の所有者がユーザ本人であることの確認ができると同時に、該媒体１から、ユーザによって記録された任意の保管情報を取り出して利用することができ、しかもその利用時に、利用者が媒体１の正しい所有者又は媒体１に上記保管情報を記録した者であることの照合がなされ、さらに記録された保管情報に改竄がないことの確認が行えるようになる。

【００９７】尚、本発明の本人確認方法、本人確認装置、媒体作成装置、媒体、媒体保管情報の処理方法、プログラム及び記録媒体は、上述の実施例にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【００９８】

【発明の効果】以上、説明したように本発明の請求項１～請求項２４記載の本人確認方法、本人確認装置、媒体作成装置、媒体、媒体保管情報の処理方法、プログラム及び記録媒体によれば、他の装置との接続が要求されることなく、媒体の記録内容を読み取らせるだけで本人確認ができるようになると共に、上記媒体上に格納されるデータは、本人確認のために入力されるデータそのものではなく、しかも該媒体上に格納されるデータからは、上記入力の要求される本人確認のためのデータの割り出しが困難なため、セキュリティも向上することになるという優れた効果を奏し得る。そのため、媒体の盗難、偽造などに対しても、極めて強力に対抗できるセキュリティを提供することができるようになり、さらに郵送中や媒体発行者の業務遂行中、或いは媒体作成中の暗証番号の盗難リスクなども回避されるようになる。

【００９９】さらに請求項１３～請求項１８、及び請求項２１～請求項２４までに記載の構成によれば、媒体の所有者が本人であることの確認ができると同時に、該媒体から、本人によって記録された任意の保管情報を取り出して利用することができ、しかもその利用時に、利用者が媒体の正しい所有者又は媒体に上記保管情報を記録した者であることの照合がなされ、さらに記録された保管情報に改竄がないことの確認が行えるようになるので、媒体に保管された情報についての信頼性を確保しながら、該保管情報による機器の操作の自動実行などの処理（上記保管情報に規定された処理）ができるようになる。

【図面の簡単な説明】

【図１】媒体作成装置２による媒体作成工程を示す説明図である。

【図２】媒体作成装置２の機能構成を示す機能ブロック図である。

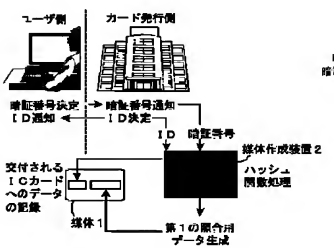
【図３】本人確認装置３における本人確認処理の工程説明図である。

【図４】本人確認装置３の機能構成を示す機能ブロック図である。
【図５】媒体作成装置２における処理の手順を示すフローチャートである。
【図６】本人確認装置３における処理の手順を示すフローチャートである。
【図７】媒体作成装置２による媒体作成工程を示す説明図である。
【図８】情報保管装置４の構成説明図である。
【図９】情報保管装置４の機能構成を示す機能ブロック図である。
【図１０】保管情報処理装置５の機能構成を示す機能ブロック図である。
【図１１】保管情報処理装置５における処理の工程説明図である。
【図１２】保管情報処理装置５における処理の手順を示すフローチャートである。

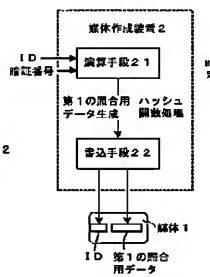
【符号の説明】

1	媒体
2	媒体作成装置
3	本人確認装置
4	情報保管装置
5	保管情報処理装置
21	演算手段
22	書込手段
31	照合用データ読取手段
32	入力手段
33	算出手段
34	照合手段
35	判定手段
41	データ読取書込手段
42	入力手段
43	第１の算出手段
44	照合手段
45	判定手段
46	第２の算出手段
51	データ読取手段
52	入力手段
53	第１の算出手段
54	第１の照合手段
55	第１の判定手段
56	第２の算出手段
57	第２の照合手段
58	第２の判定手段
59	処理手段

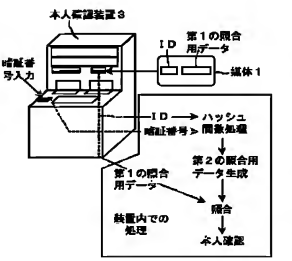
【図１】



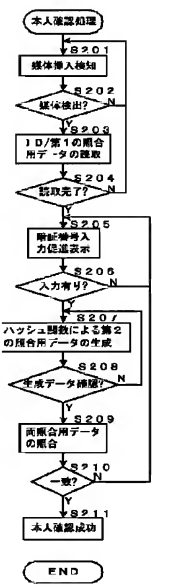
【図２】



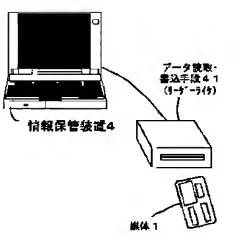
【図３】



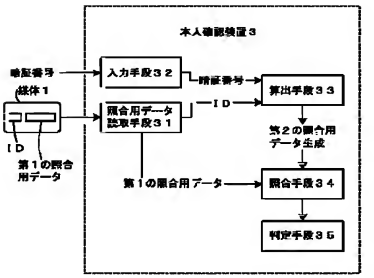
【図６】



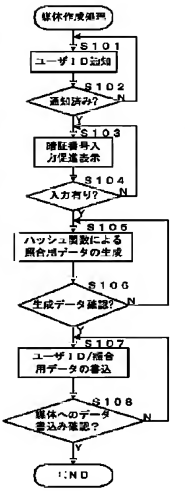
【図８】



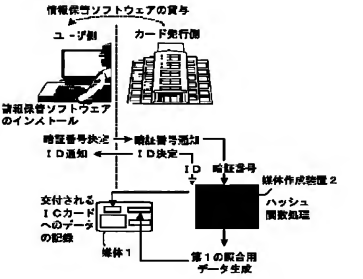
【図4】



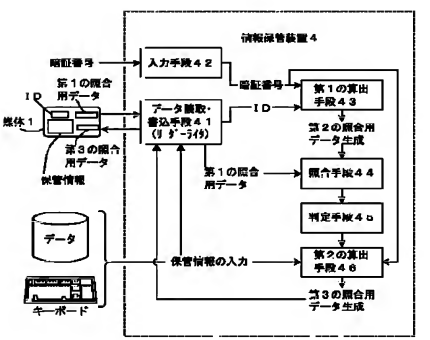
【図5】



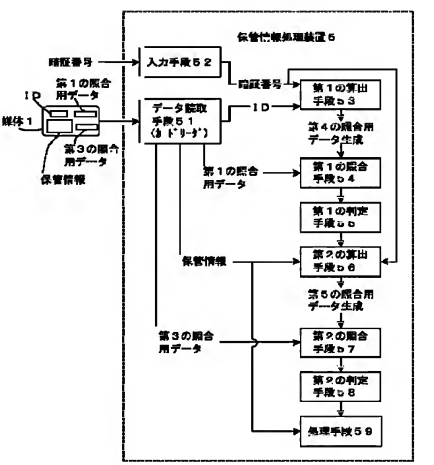
【図7】



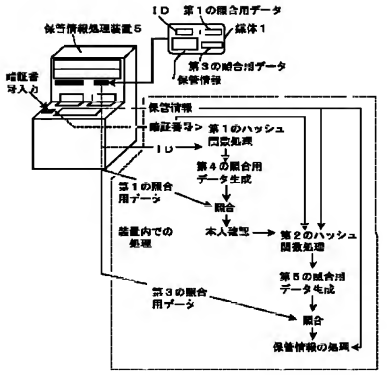
【図9】



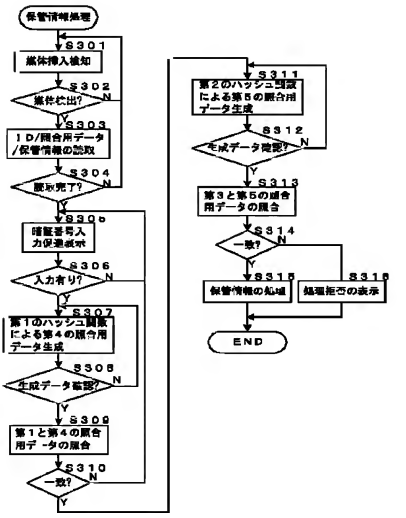
【図10】



【図11】



【図12】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
G06F 17/60	222	G06F 17/60	224	
	224	G09C 1/00	640A	
G09C 1/00	640	H04L 9/00	675A	

Fターム(参考) 2C005 HA03 HB09 HB20 JA01 JA11
MA04 MB08 NB01 SA07 SA12
SA13
5B085 AE02 AE03 AE09
5J104 AA07 AA16 EA03 EA08 KA01
KA03 NA05 NA11 NA12 NA34
NA35 PA12